<u>Amendments to the claims</u> (this listing replaces all prior versions):

1.   (currently amended) A method comprising,

in connection with authenticating a <u>supposed</u> client of a network, ~~acquiring~~ <u>receiving</u> <u>empirical</u> information that <u>represents a characterization of</u> ~~characterizes~~ the <u>supposed</u> client in a manner that enables a determination about authenticating the <u>supposed</u> client <u>as an authentic</u> <u>client</u> of the network, the information being ~~acquired~~ <u>received</u> other than ~~in the form~~ <u>as part</u> of a digital message that is passed on behalf of the <u>supposed</u> client to the network, and

making an authentication decision <u>using the received empirical information that</u> <u>represents a characterization of the supposed client and corresponding initialization information</u> <u>representing a characterization of the authentic client, the corresponding information being</u> <u>obtained other than as part of a digital message that is passed on behalf of the authentic client to</u> <u>the network</u> ~~and based on the information~~.

2.   (currently amended) The method of claim 1 in which the information <u>that</u> <u>represents the empirical characterization</u> is acquired by the network.

3.   (currently amended) The method of claim 1 in which the information <u>that</u> <u>represents the empirical characterization</u> comprises a measurable physical property of the client.

4.   (original) The method of claim 3 in which the measurable physical property is sensed from a location that is remote from the client.

5.   (original) The method of claim 3 in which the measurable physical property comprises a physical property of a device that is part of the client.

6. (original) The method of claim 3 in which the measurable physical property comprises a physical property of a person associated with the client.

7. (currently amended) The method of claim 3 in which the information that represents the empirical characterization comprises a geographic location of the client.

8. (original) The method of claim 7 in which the geographic location is determined by measuring a time of reception at multiple receiving locations of a beacon signal that originates at the client.

9. (original) The method of claim 8 in which the measurement is done at earth orbiting-satellites.

10. (original) The method of claim 8 in which the measurement is done at earth-bound receiving towers.

11. (currently amended) The method of claim 1 in which the information that represents the empirical characterization comprises a caller ID delivered by a telephone service provider.

12. (original) The method of claim 1 also including using global positioning system sources to send messages to the client.

13. (original) The method of claim 3 in which the client includes a mobile telephone device and the geographical location is determined by a mobile telephone service provider.

14.   (original) The method of claim 3 in which the measurable physical property includes internal clock phasing of the client relative to a network master clock.

15.   (original) The method of claim 1 in which the acquiring of the information is triggered by a request of the client for access to the network.

16.   (currently amended) The method of claim 1 also including

controlling access of the client to the network based on the ~~acquired~~ received information.

17.   (original) The method of claim 16 in which controlling access comprises excluding the client from access if the client has not been authenticated.

18.   (original) The method of claim 1 in which the network comprises a closed network and the location of the client is controlled by an operator of the network.

19.   (currently amended) The method of claim 1 in which a user of the client is unaware that the information that represents the actual characterization is being ~~acquired~~ received.

20.   (original) The method of claim 1 also including

sending digitized credentials from the client to the network, and

also basing the authentication decision on the digitized credentials.

21. (currently amended) A method comprising

encrypting information in a manner that is based on a physical property of an intended recipient of the information, and

delivering the encrypted information to the recipient,

the physical property decrypting the information on behalf of the recipient.

22. (original) The method of claim 21 in which the physical property comprises a location of the recipient.

23. (original) The method of claim 21 also including authenticating the recipient.

24. (canceled)

25. (currently amended) The method of claim 21 24 in which the decrypting is done automatically by the physical property.

26. (original) The method of claim 21 in which the physical property comprises a sensitivity to light or sound of a user associated with the client.

27. (original) The method of claim 21 in which the physical property of the intended recipient includes properties of DNA associated with the recipient.

28.   (original) The method of claim 21 in which the physical property of the intended recipient includes sensitivity of the recipient to light or sound.

29.   (currently amended) A method comprising

physically associating a source of a beacon with <u>an object</u> a person,

<u>periodically</u> measuring times of receipt of the beacon at multiple stations, and

determining the location <u>locations</u> of the person based on the times of receipt, and

<u>generating a map of the locations</u>.

30.   (canceled)

31.   (currently amended) The method of claim 29 also including

triggering an alert if the location <u>one of the locations</u> of the person is different from an expected location.

32.   (original) The method of claim 29 also including

performing an authentication process in connection with determining the location of the person.

33.   (currently amended) A method comprising

establishing a set of stations that are configured to ~~acquire~~ receive empirical information that <u>represents characterizations of</u> ~~characterizes~~ each of multiple <u>supposed</u> clients in a manner that enables a determination about authenticating each of the <u>supposed</u> clients <u>as an authentic</u> <u>client</u> with respect to a corresponding network, the <u>empirical</u> information being ~~acquired~~ <u>received</u> other than ~~in the form~~ <u>as part</u> of digital messages that are passed on behalf of the <u>supposed</u> clients to the corresponding networks, and

providing the <u>empirical</u> information to operators of the networks to enable them to make authentication decisions <u>using the received empirical information that represents the</u> <u>characterizations of the supposed clients and corresponding initialization information</u> <u>representing characterizations of the authentic clients, the corresponding initialization</u> <u>information being obtained other than as part of digital messages that are passed on behalf of the</u> <u>authentic clients to the network</u> ~~based on the information~~.

34.   (original) A method of encrypting and decrypting a message comprising

expressing the message as a message signal comprised of a sum based on eigenfunctions,

decomposing the sum into partial sums such that each of the partial sums conveys no meaning relative to the message, partial sums from the sum separating the expressions of the signal into partial summations,

forming electromagnetic signals based on the respective partial sums,

sending the electromagnetic signals from respective sources at times selected to assure the simultaneous arrival of the signals at an intended location, such that the electromagnetic signals superpose themselves to form the message signal.